NetSwift ASIC Packet Processor

Table of Contents

List of Figures

List of Tables

Reference Section: Detailed Description of the Preferred Embodiment
(Page 7, lines29-30; Pages 8-36, all lines)

The purpose of this application is to patent the Packet Processor bus architecture to be used for IPSec packet processing application. This bus architecture is critical in providing the efficient data flow necessary for high throughput in processing IPSec packets.

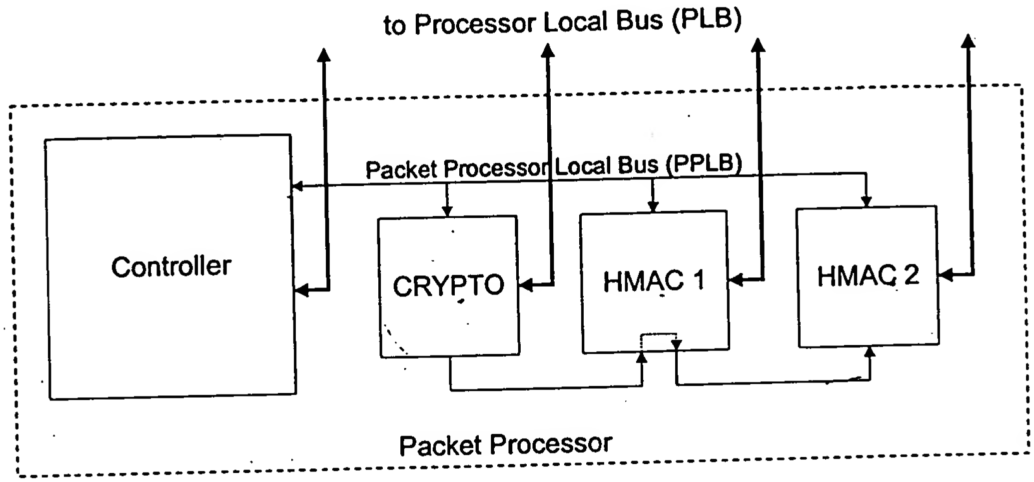

Figure 1: Packet Processor Architecture

Figure 1 shows the internal architecture of the Packet Processor. The CRYPTO unit is used to encrypt and decrypt data. HMAC 1 and HMAC 2 are authentication units. They allow the Packet Processor to perform up to two authentication on a packet. The Controller regulates the packet processing operation and fetches the input packet data for the CRYPTO, HMAC 1, and HMAC 2 units when the Packet Processor is used.

Each of the units, the Controller, CRYPTO, HMAC 1, and HMAC 2, is capable of being a bus master (i.e., being able to take over the data bus to do its own read or write transfers) for both read and write operations on the shared data bus called the Processor Local Bus or PLB. These units can also act as slave devices and be accessed by the microprocessor through the PLB bus. These bus interfaces to the PLB bus allow the CRYPTO, HMAC 1, and HMAC 2 units to be used as independent units.

When the Packet Processor is enabled, the CRYPTO, HMAC 1, and HMAC 2 units become part of the Packet Processor. The packet processing data flow is shown in Figure 2. The Controller uses its bus-master interface to read in the processing parameters and input packet data. The Controller passes processing parameters on to the CRYPTO, HMAC 1, and/or HMAC 2 units via the Packet Processor internal bus called Packet Processor Local Bus or PPLB. Depending on whether the packet is inbound or outbound and the type of processing required, the Controller passes the input packet data on to the CRYPTO, HMAC 1, and/or HMAC 2 units via the PPLB bus in the appropriate order. For outbound packets where the input payload is plaint text, the cipher text output from the CRYPTO unit is transferred to the HMAC units for authentication via the daisy chain bus. Additionally, the HMAC 1 authentication value is made available to HMAC 2 for IPSec packets requiring two authentications. Thus, with this architecture, the input packet is read once into the Packet Processor to have up to three cryptographic operations performed on the packet.

1. Packet Processor Overview

The Packet Processor consists of a RAM-based controller, one Encryption (DES/3DES/RC4) unit, and two HMAC (HMAC/SHA-1/MD5) units. The Encryption unit and the two HMAC units can operate independently when the Packet Processor is not enabled. However, when the Packet Processor is enabled, the Encryption and HMAC units become part of the Packet Processor and receive inputs from the RAM-based Controller or from the daisy chain bus, as shown in Figure 1. The Packet Processor is disabled following power-up reset.

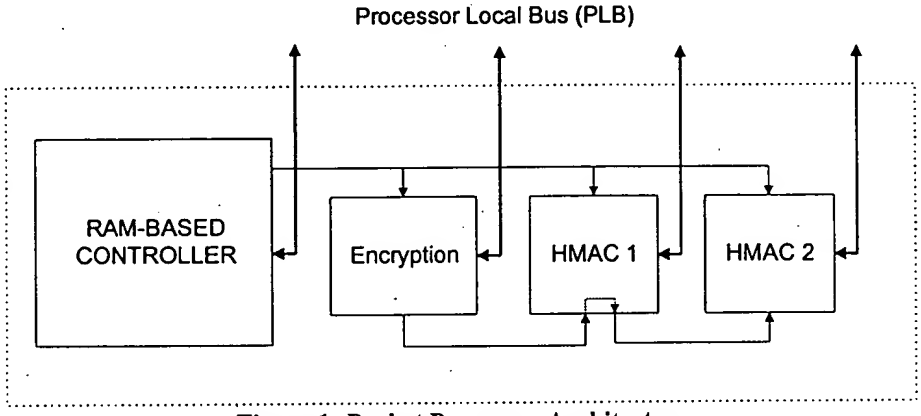

Figure 1: Packet Processor Architecture

2. RAM-based Controller

The RAM-based Controller is a programmable unit designed to control packet processing through the Encryption and HMAC units. The Controller has the following features:

- 16 dedicated internal registers
- an optimized instruction set for processing packet data
- Instruction RAM for storing up to 512 instructions
- 256-bit Mask RAM for masking out mutable fields in IP Authentication Header data
- Command FIFO for queuing up to 8 commands (one command for each packet to be processed)
- data transfer from/to memory using DMA, allowing the PPC to perform other tasks
- 16-word Input FIFO and 64-word Output FIFO
- 32-bit data bus for passing commands, parameters, and packet data to the Encryption and HMAC units
- packet processing status tagged at the end of packet output

2.1. Address Map

The RAM-based Controller dedicated registers and Mask RAM, along with registers from the Encryption and HMAC units, are address mapped to the internal Packet Processor 7-bit addressing space, as shown in Table 1. The RAM-based Controller registers and memory devices will be discussed in detail in the following section. Refer to the Encryption and HMAC sections for register definitions of those units.

Table 1: RAM-based Controller Internal Memory Map

PP Address Bus [6:0]	Device
0x00	Offset Register 0
0x01	Offset Register 1
0x02	Offset Register 2
0x03	Offset Register 3
0x04	Size Register 0
0x05	Size Register 1
0x06	Size Register 2
0x07	Size Register 3
0x08	Encryption Command Register
0x09	HMAC 1 Command Register
0x0A	HMAC 2 Command Register
0x0B	Packet Status Destination Address Register
0x0C	Offset Register 4
0x0D	Offset Register 5
0x0E	Offset Register 6
0x0F	Offset Register 7
0x15	Packet Command Register(PCR)
0x16	Base Address Register
0x17	Destination Address Register
0x18 – 0x1F	Mask RAM
0x21	Encryption RC4 Key Length Register
0x22	Encryption Key Register 0
0x23	Encryption Key Register 1

0x24	Encryption Key Register 2
0x25	Encryption Key Register 3
0x26	Encryption Key Register 4
0x27	Encryption Key Register 5
0x28	Encryption Key Register 6
0x29	Encryption Key Register 7
0x2A	Encryption DES IV Register 0
0x2B	Encryption DES IV Register 1
0x2C	Encryption Source Address Register
0x2D	Encryption Destination Address Register
0x2E	Encryption Command/Status Register
0x41	HMAC 1 Length Register 0
0x42	HMAC 1 Length Register 1
0x43	HMAC 1 Outer IV Register 0
0x44	HMAC 1 Outer IV Register 1
0x45	HMAC 1 Outer IV Register 2
0x46	HMAC 1 Outer IV Register 3
0x47	HMAC 1 Outer IV Register 4
0x48	HMAC 1 Hash Register 0
0x49	HMAC 1 Hash Register 1
0x4A	HMAC 1 Hash Register 2
0x4B	HMAC 1 Hash Register 3
0x4C	HMAC 1 Hash Register 4
0x4D	HMAC 1 Source Address Register
0x4E	HMAC 1 Destination Address Register
0x4F	HMAC 1 Command/Status Register
0x61	HMAC 2 Length Register 0
0x62	HMAC 2 Length Register 1
0x63	HMAC 2 Outer IV Register 0
0x64	HMAC 2 Outer IV Register 1
0x65	HMAC 2 Outer IV Register 2
0x66	HMAC 2 Outer IV Register 3
0x67	HMAC 2 Outer IV Register 4
0x68	HMAC 2 Hash Register 0
0x69	HMAC 2 Hash Register 1
0x6A	HMAC 2 Hash Register 2
0x6B	HMAC 2 Hash Register 3
0x6C	HMAC 2 Hash Register 4
0x6D	HMAC 2 Source Address Register
0x6E	HMAC 2 Destination Address Register
0x6F	HMAC 2 Command/Status Register

The RAM-based Controller is connected to the Processor Local Bus (PLB) as a slave device as well as a master device. The slave interface is for programming the RAM-based Controller Instruction RAM, commanding the Packet Processor, queuing up packets to be processed, and reading status. In addition, some of the RAM-based Controller internal registers may also be read via this interface. Table 2 and 3 show the PLB address map of these devices.

The RAM-based Controller is capable of becoming a master on the PLB bus, allowing it to DMA data into the Input FIFO and to DMA data out of the Output FIFO. When the master interface is not enabled, data is transferred to and from the RAM-based Controller via the slave interface.

Table 2: PLB Address Map for RAM-based Controller Registers

PLB Address	Register Name
0x20070044	Command/Status Register(CSR)
0x20070050	Configuration Register(CFG)
0x20070040	Instruction RAM Pointer Register
0x20070048	Packet Status Register (read only)
0x20070054	Packet Command Register (read only)
0x2007004C	Source Address Register (read only)
0x2007005C	Destination Address Register (read only)
0x2007002C	Packet Status Destination Address Register (read only)

Table 3: PLB Address Map for RAM-based Controller Memory Devices

PLB Address	Device Name	Size
0x20170000	Input FIFO	16 words
0x20170000	Output FIFO	64 words
0x20070060 – 0x2007007F	Mask RAM (0-7)	8 words
0x20070800 – 0x20070FFF	Instruction RAM	512 instructions
0x20171000 – 0x20171004	Command FIFO	8 commands

2.2. Instruction Set

The RAM-based Controller processes packets according to instruction routines stored in the Instruction RAM. The instruction routines are to be constructed from the instruction set described in the following sections. The instructions are 14 bits wide; the four most significant bits specify the operational code and the remaining 10 bits specify the parameters, if any, associated with the instruction. All instructions operate on 32-bit words.

2.2.1. LOAD

Operational code: 0x0
Parameter: [number of words – 10 bits wide]

This instruction causes the RAM-based Controller to load the specified number of words from the location pointed to by the Source Address Register into its Input FIFO. If input DMA is disabled, no data transfer will occur.

2.2.2. STOREX

Operational code: 0x1
Parameters: [internal address – 7 bits wide][count – 3 bits wide]

This instruction causes the RAM-based Controller to store one or multiple words from its Input FIFO to devices located at addresses beginning from the specified [internal address]. The number of words transferred is [count] plus one.

Note that storing size to Size Register 1, 2, and 3 also triggers the following operations:

- Storing size to Size Register 1 also causes (I) Encryption end offset to be computed and stored in Offset Register 5 and (ii) Encryption destination address to be computed and stored in Encryption Destination Address Register. This requires that the Destination Address Register and Offset Register 1 be initialized before writing to this size register.
- Storing size to Size Register 2 also causes (I) HMAC 1 end offset to be computed and stored in Offset Register 6 and (ii) HMAC 1 destination address to be computed and stored in HMAC 1 Destination Address Register. This requires that the Destination Address Register and Offset Register 2 be initialized before writing to this size register.
- Storing size to Size Register 3 also causes (I) HMAC 2 end offset to be computed and stored in Offset Register 7 and (ii) HMAC 2 destination address to be computed and stored in HMAC 2 Destination Address Register. This requires that the Destination Address Register and Offset Register 3 be initialized before writing to this size register.

2.2.3. START_NEW_BASE

Operational code: 0x2
Parameter: none

This instruction causes the RAM-based Controller to load the content of the Base Address Register into the Source Address Register and to start transferring data into its Input FIFO. The number of words transferred is specified by Size Register 0. If input DMA is disabled, no data transfer will occur.

Execution of this instruction also causes the output interface to be enabled (if DMA is enabled) and the byte-masking logic to be initialized.

2.2.4. WRITE

Operational code: 0x3
Parameter: [function select – 10 bits wide]

Execution of this instruction causes the selected function(s) to occur. The [function select] field is bit decoded as follow:

Bit 9-5 – **Reserved.** These bits should be set to zero.

Bit 4 – **Enable HMAC 2 Daisy Chain Input.** This bit set commands HMAC 2 to receive the remaining input data from the daisy chain bus.

Bit 3 – **Enable HMAC 1 Daisy Chain Input.** This bit set commands HMAC 1 to receive the remaining input data from the daisy chain bus.

Bit 2 – **Reset Output FIFO.** This bit set commands the RAM-based Controller to reset its Output FIFO.

Bit 1 – **Write All.** This bit set commands the RAM-based Controller to write the remaining content of its Output FIFO to memory. This command should be used only once for each packet and should be executed after all inputs into the Output FIFO are loaded. Execution of this command is required if sequential output is enabled, even if the Output FIFO is empty.

Bit 0 – **Load Packet Status Destination Address Register.** This bit set causes the destination address for the packet status to be computed and loaded into the Packet Status Destination Address Register. This must be done before executing the WRITE_DATA instruction.

2.2.5. WRITE_STATBLKCMD

Operational code: 0x4
Parameter: none

This instruction causes the RAM-based Controller to set the appropriate enable bits in the Packet Status Register to enable status reporting for the appropriate units.

2.2.6. WRITE_DATA

Operational code: 0x5
Parameters: [write configuration – 7 bits wide][offset register select – 3 bits wide]

This instruction causes the RAM-based Controller to broadcast data from the RAM-based Controller Input FIFO to the destinations specified by the write configuration. The [write configuration] field is bit decoded as follow:

Bit 6 – **Reserved.** This bit should be set to zero.

Bit 5 – **HMAC 1 ICV Write Enable.** This bit set enables writing to the HMAC 1 Expected ICV Register.

Bit 4 – **HMAC 1 Input FIFO Write Enable.** This bit set enables writing to the HMAC 1 Input FIFO.

Bit 3 – **HMAC 2 ICV Write.** This bit set enables writing to the HMAC 2 Expected ICV Register.

Bit 2 – **HMAC 2 Input FIFO Write Enable.** This bit set enables writing to the HMAC 2 Input FIFO.

Bit 1 – **Encryption Input FIFO Write Enable.** This bit set enables writing to the Encryption Input FIFO.

Bit 0 – **RAM-based Controller Output FIFO Write Enable.** This bit set enables writing to the RAM-based Controller Output FIFO.

The number of words to be transferred is indicated by the selected Offset Register. "000" in the [offset register select] field selects Offset Register 0. "111" in the [offset register select] field selects Offset Register 7. If the destination is a FIFO, the RAM-based Controller checks the corresponding FIFO full flag before writing. Byte masking for HMAC 1 and HMAC 2, if enabled, takes effect while executing this instruction. All offset registers decrement while executing this instruction.

2.2.7. WAIT

Operational code: 0x6
Parameter: [condition – 10 bits wide]

This instruction causes the RAM-based Controller to wait until the specified conditions are met. Conditions are checked only if the corresponding units are enabled (via the Packet Command Register). The [condition] field is bit-decoded as follow:

Bit 9-8 – Reserved. These bits should be set to zero

Bit 7 – HMAC 1 not busy

Bit 6 – HMAC 1 buffer not full

Bit 5 – HMAC 1 Input FIFO available

Bit 4 – HMAC 2 not busy

Bit 3 – HMAC 2 buffer not full

Bit 2 – HMAC 2 Input FIFO available

Bit 1 – Encryption not busy

Bit 0 – RAM-based Controller Output FIFO empty

This instruction should be used to verify that the Encryption unit is not busy before performing any write to it; that the HMAC buffers are not full before writing any parameter or command to the units; and that the HMAC Input FIFOs are available before writing commands to the units and loading data to the FIFOs. These conditions (bits 1-7) need to be checked once before writing data from a new packet to the corresponding units.

2.2.8. STOP

Operational code: 0x7
Parameter: none

This instruction indicates the end of a service routine. After executing this instruction, the RAM-based Controller starts to process the next command from the Command FIFO, if applicable (depending on the control bits in the Command/Status Register and the Configuration Register).

2.3. Initialization

Several operations must occur before the Packet Processor may be used. The Instruction RAM must be initialized with instruction routines to be used to process the various IPSec packets. The Configuration Registers of the RAM-based Controller, Encryption unit, and HMAC units must be set up to the desired mode and PLB bus priority (if DMA transfer will be used). Depending on the required execution mode of the Packet Processor (refer to the definition of the Command/Status Register), the Command/Status Register may be initialized at this time (for Execute Until Stop mode) to turn "ON" the Packet Processor.

2.4. Packet Processing Operation

The Packet Processor processes IPSec packets through the use of packet control structures. A packet control structure is constructed either by the host or the PPC to specify how a packet is to be processed and to pass parameters. The following is a sample list of information that may be contained in the packet control structure:

- Input packet data address and output destination address.
- Starting/ending offset of data to be encrypted or authenticated.
- Size of data to be processed in each of the units.
- RC4, DES, 3DES, HMAC 1, and/or HMAC 2 keys.
- DES, 3DES, HMAC 1, and or HMAC 2 Initial Values.
- Algorithm, Mask data, processing modes.

The order of information and parameters in the packet control structure must correspond with the instruction routine to be used to process it and its packet data. The location of the packet control structure, together with

the Instruction RAM offset of the routine, are loaded into the Command FIFO as a command for the Packet Processor. Up to eight packets may be queued in the Command FIFO for back-to-back packet processing.

When the Packet Processor is "ON", the RAM-based Controller unloads a command from the Command FIFO as soon as it finishes processing the current packet. The Instruction RAM offset is loaded to the Instruction RAM Pointer Register, and the address of the packet control structure is loaded to the Source Address Register. The RAM-based Controller then starts to execute the instruction routine pointed to by the Instruction RAM Pointer Register. Depending on the execution mode selected in the Command/Status Register, the RAM-based Controller can start processing the next command from the Command FIFO after it executes the STOP instruction of the current routine.

The Packet Processor finishes processing a packet when all of the units (Encryption, HMAC 1, and/or HMAC 2) that are required to process the packet have completed. This is indicated by the most significant bit of the Packet Status Register, which, when set, also signifies that other status bits in the register are valid for interpretation.

The Packet Processor can generate interrupts due to several conditions: (i) after each packet is processed and all outputs, including the status word, are written out to the destination, (ii) when the Command FIFO has the programmed number of spaces available, and (iii) when the Busy bit of the Command/Status Register transitions from one to zero. The Encryption and HMAC units also generate interrupts when the Busy bits of their Command/Status Registers transition from one to zero, indicating the completion of data processing. All of these critical interrupts are disabled following reset.

Note that if a packet requires utilization of more than one unit, the command registers of these units must be written in the order of Encryption Command/Status Register, followed by HMAC 1 Command/Status Register, and then HMAC 2 Command/Status Register.

2.5. Internal Calculations

The RAM-based Controller performs several calculations based on the information provided through the packet control structure. The following algorithm is used to compute the destination address for the packet status such that the packet status is appended to the end of the packet output.

For outbound packets,

If HMAC 2 is enabled, then
  Packet Status Destination Address = [Destination Address Register]+[Offset Register 7]+[HMAC 2 result size]
Else if HMAC 1 is enabled, then
  Packet Status Destination Address = [Destination Address Register]+[Size Register 0]+[HMAC 1 result size]
Else
  Packet Status Destination Address = [Destination Address Register]+[Size Register 0].

For inbound packets,

If HMAC 2 is enabled and HMAC out DMA is enabled, then
  Packet Status Destination Address = [Destination Address Register]+[Size Register 0]+[HMAC 2 result size]
Else if HMAC 1 is enabled and HMAC out DMA is enabled, then
  Packet Status Destination Address = [Destination Address Register]+[Size Register 0]+[HMAC 1 result size]
Else if Encryption is enabled, then
  Packet Status Destination Address = [Destination Address Register]+[Offset Register 5]
Else
  Packet Status Destination Address = [Destination Address Register]+[Size Register 0].

The address calculated above is used when the WRITE instruction is used to load the Packet Status Destination Address Register. The destination address may also be pre-computed and passed to the Packet Status Destination Address Register through the packet control structure by using the STOREX instruction.

Destination addresses for the Encryption, HMAC 1, and HMAC 2 units are computed as shown below and written to the Destination Address Registers of the units when Size Registers 1, 2, and 3 are loaded, respectively (refer to the description for STOREX instruction). These destination addresses may also be pre-computed and passed to these registers through the packet control structure by using the STOREX instruction with the appropriate internal addresses.

Encryption Destination Address	= [Destination Address Register]+[Offset Register 1]
HMAC 1 Destination Address	= [Destination Address Register]+[Offset Register 2]+[Size Register 2].
HMAC 2 Destination Address	= [Destination Address Register]+[Offset Register 3]+[Size Register 3].

2.6. Register Definitions

All registers internal to the RAM-based Controller are 32 bits wide, except for the Offset and Size Registers, which are 16 bits wide.

2.6.1. Configuration Register

PLB Address: 0x20070050

The bit-definition of this register is shown in Table 4. Writing to this register is allowed only when the Busy bit of the Command/Status Register is clear, except for the Terminate and Stop bits, which may be updated at any time.

Table 4: Configuration Register

Bit #	Description
31	**Terminate.** This bit set commands the Packet Processor to stop immediately. The PPC also needs to set the Terminate bits of the Encryption and HMAC units as well. This bit should be set to zero during normal operation. This bit may be updated at any time.
30	**Stop When Empty.** This bit set commands the Packet Processor to stop when all commands in the Command FIFO are processed. This bit is used only when the Execute until Stop bit of the Command/Status Register is set and DMA is enabled. This bit can be updated at any time.
29	**Stop When Done.** This bit set commands the Packet Processor to stop after it finishes processing the current command. This bit is used only when the Execute until Stop bit of the Command/Status Register is set and DMA is enabled. This bit can be updated at any time.
28:16	**Reserved.** These bits should be set to all zeroes.
15:12	**Command FIFO Interrupt Threshold.** These bits specify when, in term of the number of spaces available in the Command FIFO, to generate an interrupt. Valid values are 0 through 8.
11:9	**Reserved.** These bits should be set to all zeroes.
8	**HMAC Output DMA Enable.** This bit set specifies to always write out HMAC 1 and HMAC 2 results. This bit clear specifies to write out HMAC 1 and HMAC 2 results only when it is an outbound packet and the Output DMA Enable bit of the Command/Status Register is set.
7	**Packet Processor Enable.** This bit set enables the Packet Processor to control the Encryption and HMAC units. This bit clear disables the Packet Processor, and thus, the Encryption and HMAC units operate independent from each other and are controlled by the PPC.

6	**Instruction RAM Configuration Enable.** This bit set allows the PPC to write to the Instruction RAM. This bit clear inhibits all writing to the Instruction RAM.
5	**Reset Command FIFO.** This bit set specifies to reset the Command FIFO. This bit should be clear during normal operation.
4	**Sequential Output Disable.** This bit clear commands the Packet Processor to write out packet results sequentially. This bit set commands the Packet Processor to write out results as they become available (not necessarily sequential).
3:2	**Status Local Bus Priority.** These bits specify the priority to be used when writing out the packet status using the PLB master interface. 00 specify lowest priority; 11 specify highest priority.
1:0	**FIFO Local Bus Priority.** These bits specify the PLB bus priority to be used when performing DMA transfer of data to/from the RAM-based Controller Input and Output FIFO using the master interface. 00 specify lowest priority; 11 specify highest priority.

2.6.2. Command/Status Register

PLB Address: 0x20070044

The bit-definition of this register is shown in table 5. Writing to this register turns "ON" the Packet Processor and sets the Busy bit. Writing to this register is not allowed when the Busy bit is set.

Table 5: Command/Status Register

Bit #	Description
31	**Busy.** This read-only bit set indicates that the Packet Processor is "ON", i.e., either is idle waiting for more packets or is processing packets. This bit clear indicates that the packet processor is "OFF".
30	**Command FIFO Full.** This read-only bit set indicates the Command FIFO is full.
29	**Command FIFO Empty.** This read-only bit set indicates the Command FIFO is empty.
28	**HMAC 1 Busy.** This read-only bit set indicates that HMAC 1 is busy. This bit clear indicates that HMAC 1 is idle.
27:26	**Reserved.**
25	**HMAC 2 Busy.** This read-only bit set indicates that HMAC 2 is busy. This bit clear indicates that HMAC 2 is idle.
24:23	**Reserved.**
22	**Encryption Busy.** This read-only bit set indicates that Encryption is busy. This bit clear indicates that Encryption is idle.
21	**Controller Output FIFO Empty.** This read-only bit set indicates that the RAM-based Controller Output FIFO is empty. This bit clear indicates that the FIFO is not empty.
20:6	**Reserved.**
5:4	**Execution Mode.** These bits specify how the Packet Processor should process commands from the Command FIFO and are decoded as follow: **00 – Execute Until Stop.** The Packet Processor processes commands from the Command FIFO until one of the Stop bits in the Configuration Register is set and then clears the Busy bit.

	01 – **Execute Until Empty.** The Packet Processor processes commands from the Command FIFO until the Command FIFO becomes empty and then clears the Busy bit. 1x – **Execute One Command.** The Packet Processor executes one command from the Command FIFO and then clears the Busy bit. These bits are ignored if Input DMA is disabled.
3	**Output DMA AutoIncrement Disable.** This bit clear specifies to increment the destination address when using the PLB master interfaces to write out packet processing results. This bit set specifies not to increment the destination address.
2	**Output DMA Enable.** This bit set enables the Packet Processor to write out the results using the PLB master interfaces. This bit clear disables all PLB master write interfaces.
1	**Input DMA AutoIncrement Disable.** This bit clear specifies to increment the source address when using the PLB master interface to read in data. This bit set specifies not to increment the source address.
0	**Input DMA Enable.** This bit set enables the Packet Processor to read in data using the PLB master interface. If this bit is clear, the PPC must initializes the Instruction RAM Pointer Register, write to this register, and then loads the packet control structure and packet data to the RAM-based Controller Input FIFO for each packet.

2.6.3. Packet Command Register

PP Address: 0x15
PLB Address: 0x20070054

The Packet Command Register is used to specify how the packet should be processed. The bit definitions are shown in Table 6. This register is loaded from the Input FIFO by using the STOREX instruction. This register should be initialized first. This register may be read using the PLB address above.

Table 6: Packet Command Register

Bit #	Description
31	**HMAC 1 Mask Enable** – This bit set enables byte masking of data to be written to HMAC 1 Input FIFO. This bit clear specifies not to mask data.
30:28	**HMAC 1 Mask Size** – These bits select the number of 32-bit mask words to be applied. "000" enables byte masking of the first 32 bytes of packet data. "001" enables byte masking of the first 64 bytes of packet data. "111" enables byte masking of the first 256 bytes of packet data.
27	**HMAC 1 Initialize Hash.** This bit set specifies to use the default initial value specified by the algorithm as the starting hash value. This bit clear specifies to use the value currently in the Hash Registers as the starting hash value.
26	**HMAC 1 Final Block.** This bit set specifies to append padding and complete the hash operation. If the HMAC algorithm is selected, the unit will also perform the outer hash. This bit clear specifies that this is not the last block of the message and no padding or length should be appended. Note that size must be multiples of 512 bits if this bit is not set.
25:24	**HMAC 1 Algorithm.** These bits specify the algorithm to be performed and are decoded as follow: 00 -- MD5 01 -- SHA-1 10 -- HMAC-MD5

	11 -- HMAC-SHA-1
23	**HMAC 2 Mask Enable** – This bit set enables byte masking of data to be written to HMAC 2 Input FIFO. This bit clear specifies not to mask data.
22:20	**HMAC 2 Mask Size** – These bits select the number of 32-bit mask words to be applied. "000" enables byte masking of the first 32 bytes of packet data. "001" enables byte masking of the first 64 bytes of packet data. "111" enables byte masking of the first 256 bytes of packet data.
19	**HMAC 2 Initialize Hash**. This bit set specifies to use the default initial value specified by the algorithm as the starting hash value. This bit clear specifies to use the value currently in the Hash Registers as the starting hash value.
18	**HMAC 2 Final Block**. This bit set specifies to append padding and complete the hash operation. If the HMAC algorithm is selected, the unit will also perform the outer hash. This bit clear specifies that this is not the last block of the message and no padding or length should be appended. Note that size must be multiples of 512 bits if this bit is not set.
17:16	**HMAC 2 Algorithm**. These bits specify the algorithm to be performed and are decoded as follow: 00 -- MD5 01 -- SHA-1 10 -- HMAC-MD5 11 -- HMAC-SHA-1
15	**HMAC 1 Length/IPAD/OPAD** Select. When the Initialize Hash bit is set and the Final Block bit is clear, this bit is used to select between HMAC IPAD and OPAD. This bit set specifies to use the HMAC IPAD; this bit clear specifies to use the HMAC OPAD. This bit is used when performing the HMAC Inner and Outer IV generation commands. Otherwise, this bit is used to select the source of the message length. This bit set specifies to use the contents of the Length Registers as the length of the message; this bit clear specifies to use the Size field as the length of the message.
14	**HMAC 2 Length/IPAD/OPAD** Select. When the Initialize Hash bit is set and the Final Block bit is clear, this bit is used to select between HMAC IPAD and OPAD. This bit set specifies to use the HMAC IPAD; this bit clear specifies to use the HMAC OPAD. This bit is used when performing the HMAC Inner and Outer IV generation commands. Otherwise, this bit is used to select the source of the message length. This bit set specifies to use the contents of the Length Registers as the length of the message; this bit clear specifies to use the Size field as the length of the message.
13	**HMAC using HMAC 1 and HMAC 2**. This bit set specifies to use both HMAC units to perform the HMAC Final command. Note that HMAC 2 offsets and size should be the same as HMAC 1 offsets and size when performing this operation. If this is an inbound packet, the expected authentication value should be loaded to the HMAC 2 ICV Registers. This bit clear specifies to perform the entire HMAC operation using one HMAC unit.
12	**Encryption 3DES Keys for Decryption/Initialize RC4.** When Encryption unit is set to perform a 3DES operation, this bit specifies whether the 3DES key is for encryption or decryption. This bit set specifies that keys 1,2, and 3 are in the order for decryption and that the order of the keys should be reversed if encryption mode is selected. This bit clear specifies that keys 1,2, and 3 are in the order for encryption and that the order of the keys should be reversed if decryption mode is selected. Otherwise, this bit specifies whether RC4 initialization should be performed. This bit set specifies to initialize the RC4 engine with the key loaded in the Encryption Key Registers. This bit clear

	specifies to use the key stream that is currently in the RC4 engine.

11:8	**Encryption Algorithm[3:0]**. These bits specify the algorithm to be performed and are decoded as follow:
	bit 3: 1= RC4 0=DES/3DES;
	bit 2: 1= 3DES 0= DES;
	bit 1: 1= ECB 0= CBC;
	bit 0: 1= decryption 0= encryption

7	**Reserved.** This bit should be set to zero.
6	**Encryption Enable.** This bit set indicates that the Encryption unit is required for the processing of this packet. This bit clear indicates that the Encryption unit is not required for the processing of this packet.
5	**HMAC 1 Enable.** This bit set indicates that the HMAC 1 unit is required for the processing of this packet. This bit clear indicates that the HMAC 1 unit is not required for the processing of this packet.
4	**HMAC 2 Enable.** This bit set indicates that the HMAC 2 unit is required for the processing of this packet. This bit clear indicates that the HMAC 2 unit is not required for the processing of this packet.
3:2	**Mode Select.** These bits specify the size of the authentication value and the selection is applied to both HMAC units. 00 – selects to use only the leftmost 96 bits. 01 – selects to use only the leftmost 128 bits. 1x – selects to use the entire authentication value (160 bits for SHA-1, 128 bits for MD5).
1	**Inbound Packet.** This bit set indicates that this is an inbound packet. This bit clear indicates that this is an outbound packet.
0	**Endian.** This bit set specifies that the packet data to be processed is in little endian format. This bit clear specifies that the packet data to be processed is in big endian format. This bit also specifies the endian format for outputs from the packet processor, except for the packet status.

2.6.4. Base Address Register

PP Address: 0x016

This register specifies the source address of the input packet data to be processed. This register is loaded from the Input FIFO by using the STOREX instruction.

2.6.5. Destination Address Register

PP Address: 0x017
PLB Address: 0x2007005C

This register specifies the destination address where the Packet Processor output will be written. This register is loaded from the Input FIFO by using the STOREX instruction. This register may be read using the PLB address above.

2.6.6. Offset Registers 0-7

PP Addresses: 0x00, 0x01, 0x02, 0x03, 0x0C, 0x0D, 0x0E, 0x0F

An input packet may compose of an IP header, an AH header, an ESP header, a payload, authentication data, etc... Since the various segments in a packet may not be processed the same way, eight Offset Registers are provided for specifying the offsets of the starting or ending of certain data segment. Offset Registers 1, 2, and 3 may be used to store the starting offset for data segments to be processed in the Encryption, HMAC1, and HMAC2 units, respectively. Similarly, Offset Registers 5, 6, and 7 may be used for the ending offsets.

The Offset Registers are 16 bits wide and indicate the number of bytes from the beginning of a packet. They are loaded from the 16 least significant bits of the Input FIFO by using the STOREX instruction. The Offset Registers 5, 6, and 7 are also loaded automatically with the internally computed values when Size Registers 1, 2, and 3 are loaded, respectively. Refer to the STOREX instruction description for more details. All non-zero Offset Registers decrement when the WRITE_DATA instruction is executed. Note that since all data are on 32-bit boundary, the two least significant bits are ignored.

2.6.7. Size Registers 0-3

PP Addresses: 0x04, 0x05, 0x06, 0x07

Size Register 0 specifies the total number of bytes in the packet data, while Size Registers 1-3 specify the size of the data to be processed in the Encryption, HMAC 1, and HMAC 2 units, respectively.

The Size Registers are 16 bits wide and are loaded from the 16 least significant bits of the Input FIFO by using the STOREX instruction. Since data is multiples of 32-bit words, the two least significant bits are ignored.

2.6.8. Encryption Command Register

PP Address: 0x08

The Encryption Command Register is the command register in the Encryption unit, also known as the Encryption Command/Status Register at PP address 0x2E. When this register is loaded using the PP address 0x08, the command is derived from the information specified in the RAM-based Controller Packet Command Register, Command/Status Register, Configuration Register, and the Size Registers.

2.6.9. HMAC 1 Command Register

PP Address: 0x09

The HMAC 1 Command Register is the command register in the HMAC 1 unit, also known as HMAC 1 Command/Status Register at PP address 0x4F. When this register is loaded using the PP address 0x09, the command is derived from the information specified in the RAM-based Controller Packet Command Register, Command/Status Register, Configuration Register, and the Size Registers.

2.6.10. HMAC 2 Command Register

PP Address: 0x0A

The HMAC 2 Command Register is the command register in the HMAC 2 unit, also known as the HMAC 2 Command/Status Register at PP address 0x6F. When this register is loaded using the PP address 0x0A, the command is derived from the information specified in the RAM-based Controller Packet Command Register, Command/Status Register, Configuration Register, and the Size Registers.

2.6.11. Packet Status Destination Address Register

PP Address: 0x0B
PLB Address: 0x2007002C

This register stores the destination address for the status that is generated at the end of a packet processing. This register is loaded from the Input FIFO by using the STOREX instruction or from the internally computed address by using the WRITE instruction. This register may be read using the PLB address above.

2.6.12. Packet Status Register

PLB Address: 0x20070048

This read-only register reports the status of the packet being processed. The enable bits are set by the RAM-based Controller, and the status bits are set as the conditions become true. The most significant bit is set when processing of the packet has completed. If output DMA is enabled, the content of this register is written out to the address specified in the Packet Status Destination Address Register. The bit-definition of this register is shown in Table 7.

Table 7: Packet Status Register

Bit #	Description
31	**Completed packet processing.** This bit set indicates that packet processing has completed and all status bits in this register are valid. This bit clear indicates that packet processing has not completed and status bits in this register should be ignored.
30:24	**Reserved.** Read as zero.
23	**Encryption Status Enable.** This bit set specifies to report status for the Encryption unit. This bit clear specifies not to report status for the Encryption unit.
22	**Encryption Done.** This bit set indicates that the Encryption unit has completed processing. This bit clear indicates that the Encryption unit has not completed processing. This bit should be ignored when the Encryption Status Enable bit is low.
21	**Encryption Key error.** When the Encryption unit is set to perform an RC4 operation, this bit set indicates that the key length is 0 or greater than 32 bytes. This bit clear indicates that the key length is valid. Otherwise, this bit set indicates that the keys (key 1 for DES; keys 1, 2, and 3 for 3DES) contain parity error. This bit clear indicates that each byte of the keys has odd parity. Note that key errors do not stop the packet from being processed. This bit should be ignored when the Encryption Status Enable bit is low.
20:16	**Reserved.** Read as zero.
15	**HMAC 2 Status Enable.** This bit set specifies to report status for the HMAC 2 unit. This bit clear specifies not to report status for the HMAC 2 unit.
14	**HMAC 2 Done.** This bit set indicates that the HMAC 2 unit has completed processing. This bit clear indicates that the HMAC 2 unit has not completed processing. This bit should be ignored when the HMAC 2 Status Enable bit is low.
13	**HMAC 2 Size Error.** This bit set indicates that the data size is not an even multiple of 64 bytes when performing the HMAC/hash update command and that the result should be discarded. This bit clear indicates that the data size is valid. This bit should be ignored when the HMAC 2 Status Enable bit is low.
12	**HMAC 2 ICV Check Enable.** This bit set specifies to compare HMAC 2 result with the expected authentication value from the inbound packet.
11	**HMAC 2 ICV Check Status.** This bit set indicates that the HMAC 2 result matches with the expected authentication value. This bit clear indicates that the comparison failed. This bit should be ignored when the HMAC 2 ICV Check Enable bit is low.

10:8	**Reserved.** Read as zero.
7	**HMAC 1 Status Enable.** This bit set specifies to report status for the HMAC 1 unit. This bit clear specifies not to report status for the HMAC 1 unit.
6	**HMAC 1 Done.** This bit set indicates that the HMAC 1 unit has completed processing. This bit clear indicates that the HMAC 1 unit has not completed processing. This bit should be ignored when the HMAC 1 Status Enable bit is low.
5	**HMAC 1 Size Error.** This bit set indicates that the data size is not an even multiple of 64 bytes when performing the HMAC/hash update command and that the result should be discarded. This bit clear indicates that the data size is valid. This bit should be ignored when the HMAC 1 Status Enable bit is low.
4	**HMAC 1 ICV Check Enable.** This bit set specifies to compare HMAC 1 result with the expected authentication value from the inbound packet.
3	**HMAC 1 ICV Check Status.** This bit set indicates that the HMAC 1 result matches with the expected authentication value. This bit clear indicates that the comparison failed. This bit should be ignored when the HMAC 1 ICV Check Enable bit is low.
2 : 0	**Reserved.** Read as zero.

2.6.13. Instruction RAM Pointer Register

PLB Address: 0x20070040

This 9-bit register stores the pointer to the instruction routine in the Instruction RAM to be used to process the packet. This register loads from the nine least significant bits of the PLB data bus and advances as the RAM-based Controller executes the instructions.

This register is initialized by the PPC only when the input DMA is disabled. Otherwise, this register is loaded by the RAM-based Controller with data from the Command FIFO.

2.6.14. Source Address Register

PLB Address: 0x2007004C

This register is used internal to the RAM-based Controller to buffer the source address for the input packet control structure and data. This register may be read using the PLB address above.

2.7. Mask RAM

PP Addresses: 0x18 – 0x1F
PLB Address: 0x20070060 – 0x2007007F

The Mask RAM stores mask data for the first 256 bytes of packet data. The RAM may be loaded either by the PPC via the PLB slave bus or by the RAM-based Controller via the STOREX instruction. The application of the mask data to HMAC 1 and/or HMAC 2 Input FIFO data is controlled by information in the Packet Command Register.

The Mask RAM is 8 deep and 32 bits wide. The format of the Mask RAM is shown in Figure 2 below (for the first Mask RAM location). The masking data is for packet data in big endian format. If the packet data is in little endian format, the RAM-based Controller will swap the bits.

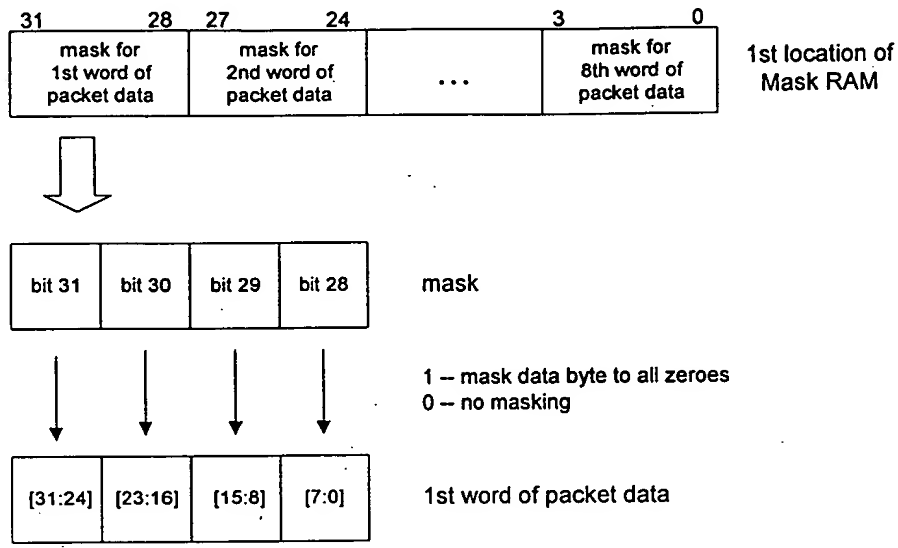

Figure 2: Mask RAM Format

2.8. Instruction RAM

PLB Address: 0x20070800 – 0x20070FFF

Instruction routines constructed from the instruction set are stored in the Instruction RAM. The Instruction RAM can store up to 512 instructions and must be initialized before the Packet Processor is used. The Instruction RAM loads from the lower 14 bits of the PLB slave bus when writing to the PLB address above while the Instruction RAM Configuration Enable bit of the Configuration Register is set.

2.9. Command FIFO

PLB Addresses: 0x20171000 – 0x20171004

For each packet to be processed by the Packet Processor, the PPC must enter a command into the Command FIFO via the PLB slave interface to specify the instruction routine to be used and the location of the packet control structure. The Instruction RAM offset is temporarily stored in a register at PLB address 0x20171000. When the address of the packet control structure is written to PLB address 0x20171004, the entire command is entered into the Command FIFO. Reading the Command FIFO via the PLB slave interface returns the next command to be processed (without unloading the FIFO).

The Command FIFO is unloaded by the RAM-based Controller as soon as the Controller finishes processing the current packet. The Instruction RAM offset is loaded to the Instruction RAM Pointer Register and the address of the packet control structure is loaded to the Source Address Register. The RAM-based Controller then starts to execute the instruction routine pointed to by the Instruction RAM Pointer Register.

The Command FIFO can store up to eight commands. Its status flags can be read via the Command/Status Register. The Command FIFO can also generate an interrupt when the number of spaces available equals the threshold set in the Configuration Register. Resetting the Command FIFO may be done by setting bit 5 of the Configuration Register.

2.10. Input and Output FIFO

PLB Address: 0x20170000

The RAM-based Controller Input FIFO and Output FIFO may be accessed using the PLB address above. Data may also be transferred to/from the FIFOs using the PLB master interfaces, when DMA is enabled. Data is written into the Input FIFO. Data is read from the Output FIFO.

3. Encryption Unit

The Encryption unit supports DES in CBC and ECB modes, triple DES (3DES) in outer CBC and ECB modes, and RC4. The unit can encrypt at the rate of 528 Mbps for DES, 176 Mbps for 3DES, and 528 Mbps for RC4. Table 8 shows the encryption commands that are available from this unit.

Table 8: Encryption Unit Commands

Command	Description
DES CBC Complete	Perform complete DES CBC encryption or decryption.
DES ECB Complete	Perform complete DES ECB encryption or decryption.
3DES CBC Complete	Perform complete 3DES outer CBC encryption or decryption.
3DES ECB Complete	Perform complete 3DES ECB encryption or decryption.
RC4 Complete	Perform complete RC4 encryption or decryption.
RC4 Without Initialization	Perform RC4 encryption or decryption without initialization (continue from the previous processing).

The Encryption unit is connected to the Processor Local Bus (PLB) as a slave device as well as a master device. The slave interface may be used to access all registers, the 16-word Input FIFO, and the 32-word Output FIFO internal to the unit, while the master interface provides for the more efficient DMA transfer of data to/from the Input and Output FIFOs. When the Packet Processor is enabled, the Encryption unit accepts inputs only from the RAM-based Controller, except for the Encryption Configuration Register.

The Encryption unit starts processing data following a write to the Encryption Command/Status Register. While the unit is busy encrypting or decrypting, the Busy bit of the Encryption Command/Status Register is set to one. When processing completes, the Busy bit transitions from one to zero and a maskable critical interrupt is generated.

3.1. Address Map

The Encryption unit registers and memory devices are memory-mapped to the PLB address bus as shown in Table 9. All of the Encryption unit registers, except for the Encryption Configuration Register, are also memory mapped to the Packet Processor address bus, as shown in Table 1.

Table 9: PLB Address Map for the Encryption Unit

PLB Address	Device
0x20060200	Encryption Configuration Register
0x20060204	Encryption RC4 Key Length Register
0x20060208	Encryption Key Register 0
0x2006020C	Encryption Key Register 1
0x20060210	Encryption Key Register 2
0x20060214	Encryption Key Register 3
0x20060218	Encryption Key Register 4

0x2006021C	Encryption Key Register 5
0x20060220	Encryption Key Register 6
0x20060224	Encryption Key Register 7
0x20060228	Encryption DES IV Register 0
0x2006022C	Encryption DES IV Register 1
0x20060230	Encryption Source Address Register
0x20060234	Encryption Destination Address Register
0x20060238	Encryption Command/Status Register
0x20160000	Encryption Input FIFO
0x20160000	Encryption Output FIFO

3.2. Register Definitions

All registers internal to the Encryption unit are 32 bits wide, unless specified otherwise.

3.2.1. Encryption Configuration Register

PLB Address: 0x20060200

The bit-definition of this register is shown in table 10. This register may be updated at any time.

Table 10: Encryption Configuration Register

Bit #	Description
26:25	**Local Bus Priority.** These bits specify the PLB bus priority to be used when performing DMA transfer using the master interface. 00 specify lowest priority; 11 specify highest priority.
24	**Terminate.** This bit set commands the Encryption unit to stop immediately. This bit should be set to zero during normal operation.

3.2.2. Encryption Command/Status Register

PP Address: 0x2E
PLB Address: 0x20060238

The bit-definition of this register is shown in Table 11. Writing to this register starts the Encryption unit and sets the Busy bit. Writing to this register is inhibited while the Busy bit is set. The completion of processing is indicated by the transition of the Busy bit from one to zero.

Table 11: Encryption Command/Status Register

Bit #	Description
31	**Busy.** This read-only bit set indicates that the Encryption unit is busy processing data. This bit clear indicates that the Encryption unit is idle and is ready for a new command.
30	**RC4 Initialization Busy.** This read-only bit set indicates that RC4 is initializing. This bit clear indicates that RC4 initialization is not in progress.
29	**Encryption Key error.**

	When the Encryption unit is set to perform an RC4 operation, this bit set indicates that the key length is 0 or greater than 32 bytes. This bit clear indicates that the key length is valid. Processing will continue to completion, even though the resulting text should be discarded. Otherwise, this bit set indicates that the keys (key 1 for DES; keys 1, 2, and 3 for 3DES) contain parity error. This bit clear indicates that each byte of the keys has odd parity. This error does not stop the data from being processed.
28	**Output-To-HMAC 1 Enable.** This bit set commands the Encryption unit to pass the resulting text to HMAC 1.
27	**Output-To-HMAC 2 Enable.** This bit set commands the Encryption unit to pass the resulting text to HMAC 2.
26	**Output DMA AutoIncrement Disable.** This bit clear specifies to increment the destination address when using the PLB master interface to write out the results. This bit set specifies not to increment the destination address.
25	**Output DMA Enable.** This bit set specifies to write out the results using the PLB master interface. This bit clear disables the PLB master write interface.
24	**3DES Keys for Decryption.** This bit set specifies that keys 1,2, and 3 are in the order for decryption and that the order of the keys should be reversed if encryption mode is selected. This bit clear specifies that keys 1,2, and 3 are in the order for encryption and that the order of the keys should be reversed if decryption mode is selected.

23:20	**Encryption Algorithm[3:0].** These bits specify the algorithm to be performed and are decoded as follow:
	bit 3: 1= RC4 0=DES/3DES;
	bit 2: 1= 3DES 0= DES;
	bit 1: 1= ECB 0= CBC;
	bit 0: 1= decryption 0= encryption

19	**Initialize RC4.** This bit set specifies to initialize the RC4 engine with the key loaded in the Encryption Key Registers. This bit clear specifies to use the key stream that is currently in the RC4 engine.
18	**Input DMA AutoIncrement Disable.** This bit clear specifies to increment the source address when using the PLB master interface to read in data. This bit set specifies not to increment the source address.
17	**Input DMA Enable.** This bit set specifies to read in data using the PLB master interface. This bit clear disables the PLB master read interface.
16	**Endian.** This bit set specifies that the data is in little endian format. This bit clear specifies that the data is in big endian format.
15:0	**Size.** These bits specify the number of bytes to be processed. This field is initialized when this register is updated. During processing, this field is updated to reflect the number of bytes remaining to be processed. For DES and 3DES, data size must be an integral of 64-bit words.

3.2.3. Encryption Source Address Register

PP Address: 0x2C
PLB Address: 0x20060230

This 32-bit register stores the source address of the Encryption unit input data. This register is used when input DMA is enabled and the Packet Processor is disabled.

3.2.4. Encryption Destination Address Register

PP Address: 0x2D
PLB Addresses: 0x20060234

This 32-bit register stores the destination address for the Encryption unit output data. This register is used when output DMA is enabled.

3.2.5. Encryption RC4 Key Length Register

PP Address: 0x21
PLB Address: 0x20060204

This 6-bit register stores the RC4 key length in number of bytes. The maximum key length supported is 32 bytes. Register access is not allowed while the RC4 Initialization Busy bit is high.

3.2.6. Encryption Key Registers 0-7

PP Addresses: 0x22 – 0x29
PLB Addresses: 0x20060208 – 0x20060224

These eight 32-bit registers store the key for RC4, DES, and 3DES encryption. The Encryption Key Register 0 holds the most significant word of the key string, with the leftmost character of the key in the 31:24 bit position. Register access is not allowed when the RC4 Initialization Busy bit is high.

For DES and 3DES, key 1 is stored in Encryption Key Registers 0 and 1, key 2 is stored in Encryption Key Registers 2 and 3, and key 3 is stored in Encryption Key Registers 4 and 5. Each 64-bit key is loaded into the DES/3DES engine when the register with the higher address is updated.

3.2.7. Encryption DES IV Registers 0-1

PP Addresses: 0x2A, 0x2B
PLB Addresses: 0x20060228, 0x2006022C

These two 32-bit registers store the Initialization Vector for DES and 3DES in CBC mode. The Encryption DES IV Register 0 holds the most significant 32-bit word, with the leftmost character of the vector in the 31:24 bit position.

3.3. Encryption Input and Output FIFO

PLB Address: 0x20160000

The Encryption Input FIFO and Output FIFO may be accessed using the PLB address above. Data may also be transferred to/from the FIFOs using the PLB master interface, when DMA is enabled. When the Packet Processor is used, the Input FIFO accepts data only from the RAM-based Controller, through the use of the WRITE_DATA instruction. Data is written into the Input FIFO. Data is read from the Output FIFO.

4. HMAC 1 and HMAC 2

Two HMAC units are provided to authenticate ESP (Encapsulating Security Payload) and AH (Authentication Header) data in a single pass through the Packet Processor. The units are basically the same, with a few differences, and are called HMAC 1 and HMAC2. The HMAC 1 and HMAC 2 units support keyed-hashing for message authentication and hash algorithms SHA-1 and MD5. Each of the units can hash at the rate of 417 Mbps for SHA-1 and 519 Mbps for MD5.

The commands available from the HMAC units are shown in Table 12. Commands are provided to perform the HMAC operation in one or several steps. Figure 3 shows how the operation is divided. Depending on the application, a performance improvement may be achieved by storing the intermediate Inner and Outer IV and then using them for the next message that utilizes the same key. Performance may be improved further when the packet requires only one HMAC operation. Provision is made to perform the HMAC Final command using both HMAC 1 and HMAC 2 units, one to complete the inner hash operation and the other to complete the outer hash operation.

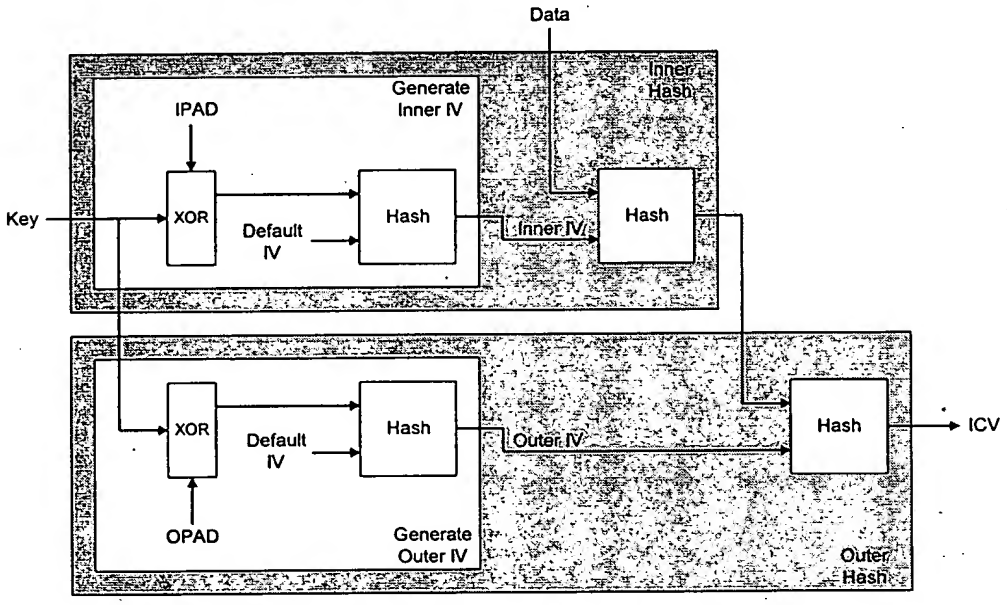

Figure 3: HMAC Operation

Table 12: HMAC Unit Commands

Command	Description
HMAC Complete	Perform complete HMAC operation (support key size of 160 bits for SHA-1 and 128 bits for MD5 only).
HMAC Inner IV Generation	Generate Inner IV.
HMAC Outer IV Generation	Generate Outer IV.
HMAC Update	Hash data using the provided Inner IV or intermediate result from a previous update command.

HMAC Final	Hash data, with padding appended, using the provided Inner IV or intermediate result from a previous update command, and then perform the outer hash using the provided Outer IV.
Hash Complete	Perform complete hash operation.
Hash Initialization & Update	Initialize with hash default IV and then hash data
Hash Final	Hash data, with padding appended, using the provided intermediate result from a previous update command.

Each of the HMAC units also has a set of Expected ICV Registers for storing the expected authentication value. When the Packet Processor is used, the HMAC units compare the final hash results against the expected values and report status for inbound packets.

The HMAC units are connected to the Processor Local Bus (PLB) as a slave device as well as a master device. The slave interfaces may be used to access all registers internal to the units, the 32-word HMAC 1 Input FIFO, and the 64-word HMAC 2 Input FIFO. The master interfaces provide for the more efficient DMA transfer of data to the Input FIFOs and of the authentication results (also known as Integrity Check Value or ICV) out from the Hash Registers. When the Packet Processor is enabled, the HMAC units accept inputs only from the RAM-based Controller, except for the HMAC 1 and HMAC 2 Configuration Registers.

Each HMAC unit starts processing data following a write to its HMAC Command/Status Register. While the unit is busy hashing, the Busy bit of the HMAC Command/Status Register is set to one. When processing completes, the Busy bit transitions from one to zero and a maskable critical interrupt is generated.

4.1. Address Map

The HMAC 1 and HMAC 2 registers and memory devices are memory-mapped to the PLB address bus as shown in Table 13. All of the registers, except for the HMAC 1 and HMAC 2 Configuration Registers, are also memory mapped to the Packet Processor address bus, as shown in Table 1.

Table 13: PLB Address Map for the HMAC Units

PLB Address	Device
0x20040000	HMAC 1 Configuration Register
0x20040004	HMAC 1 Length Register 0
0x20040008	HMAC 1 Length Register 1
0x2004000C	HMAC 1 Outer IV Register 0
0x20040010	HMAC 1 Outer IV Register 1
0x20040014	HMAC 1 Outer IV Register 2
0x20040018	HMAC 1 Outer IV Register 3
0x2004001C	HMAC 1 Outer IV Register 4
0x20040020	HMAC 1 Hash Register 0
0x20040024	HMAC 1 Hash Register 1
0x20040028	HMAC 1 Hash Register 2
0x2004002C	HMAC 1 Hash Register 3
0x20040030	HMAC 1 Hash Register 4
0x20040034	HMAC 1 Source Address Register

0x20040038	HMAC 1 Destination Address Register
0x2004003C	HMAC 1 Command/Status Register
0x20140000	HMAC 1 Input FIFO
0x20050000	HMAC 2 Configuration Register
0x20050004	HMAC 2 Length Register 0
0x20050008	HMAC 2 Length Register 1
0x2005000C	HMAC 2 Outer IV Register 0
0x20050010	HMAC 2 Outer IV Register 1
0x20050014	HMAC 2 Outer IV Register 2
0x20050018	HMAC 2 Outer IV Register 3
0x2005001C	HMAC 2 Outer IV Register 4
0x20050020	HMAC 2 Hash Register 0
0x20050024	HMAC 2 Hash Register 1
0x20050028	HMAC 2 Hash Register 2
0x2005002C	HMAC 2 Hash Register 3
0x20050030	HMAC 2 Hash Register 4
0x20050034	HMAC 2 Source Address Register
0x20050038	HMAC 2 Destination Address Register
0x2005003C	HMAC 2 Command/Status Register
0x20150000	HMAC 2 Input FIFO

4.2. Register Definitions

4.2.1. HMAC Configuration Register

HMAC 1 PLB Address: 0x20040000
HMAC 2 PLB Address: 0x20050000

The bit-definition of this register is shown in Table 14. This register can be updated at any time.

Table 14: HMAC Configuration Register

Bit #	Description
26:25	**Local Bus Priority.** These bits specify the PLB bus priority to be used when performing DMA transfer using the master interface. 00 specify lowest priority; 11 specify highest priority.
24	**Terminate.** This bit set commands the HMAC unit to stop immediately. This bit should be set to zero during normal operation.

4.2.2. HMAC Command/Status Register

HMAC 1 PP Address: 0x4F
HMAC 1 PLB Address: 0x2004003C

HMAC 2 PP Address: 0x6F
HMAC 2 PLB Address: 0x2005003C

The bit-definition of this register is shown in Table 15. Writing to this register starts the HMAC unit and sets the Busy bit. Writing to this register is inhibited while the Busy bit is set. The completion of processing is indicated by the transition of the Busy bit from one to zero.

Table 15: HMAC Command/Status Register

Bit #	Description
31	**Busy.** This read-only bit set indicates that the HMAC unit is busy processing data. This bit clear indicates that the HMAC unit is idle and is ready for a new command.
30	**Size Error.** This bit set indicates that the data size is not an even multiple of 64 bytes when performing the HMAC/hash update command and that the result should be discarded. This bit clear indicates that the data size is valid.
29:28	**Mode Select.** These bits specify the size of the authentication value. 00 – selects to use only the leftmost 96 bits. 01 – selects to use only the leftmost 128 bits. 1x – selects to use the entire authentication value (160 bits for SHA-1, 128 bits for MD5).
27	**HMAC inner/outer hash only.** For HMAC 1, this bit set specifies to perform the inner hash of HMAC only. For HMAC 2, this bit set specifies to perform the outer hash of HMAC only. This bit is used when performing the HMAC Final command using both HMAC 1 and HMAC 2.
26	**Output DMA AutoIncrement Disable.** This bit clear specifies to increment the destination address when using the PLB master interface to write out the results. This bit set specifies not to increment the destination address.
25	**Output DMA Enable.** This bit set specifies to write out the results using the PLB master interface. This bit clear disables the PLB master write interface.
24	**Output-To-HMAC 2 Enable / Input FIFO Early Release Enable.** This bit should be set to zero when the HMAC units are used as independent units. When the Packet Processor is enabled, this bit has different definitions for HMAC 1 and HMAC 2. The RAM-based Controller will set this bit accordingly when this register is loaded using PP address 0x09 0r 0x0A. Output-To-HMAC 2 Enable. This bit set in HMAC 1 specifies to pass the hash value to HMAC 2, using the daisy chain bus. This bit clear specifies not to pass the hash value. The number of words transferred is selected by the algorithm bits Input FIFO Early Release Enable. This bit set in HMAC 2 specifies to release the Input FIFO as soon as possible. This bit should be set to zero when processing inbound packets.
23	**Initialize Hash.** This bit set specifies to use the default initial value specified by the algorithm as the starting hash value. This bit clear specifies to use the value currently in the HMAC Hash Registers as the starting hash value.
22	**Final Block.** This bit set specifies to append padding and complete the hash operation. If the HMAC algorithm is selected, the unit will also perform the outer hash. This bit clear specifies that this is not the last block of the message and no padding or length should be appended. Note that size must be multiples of 512 bits if this bit is not set.
21:20	**Algorithm.** These bits specify the algorithm to be performed and are decoded as follow: 00 -- MD5 01 -- SHA-1 10 -- HMAC-MD5 11 -- HMAC-SHA-1
19	**Length/IPAD/OPAD Select.** When the Initialize Hash bit is set and the Final Block bit is clear, this bit is used to select between HMAC IPAD and OPAD. This bit set specifies to use the HMAC IPAD; this bit clear specifies to use the HMAC OPAD. This bit is used when performing the HMAC Inner and Outer IV

	generation commands. Otherwise, this bit is used to select the source of the message length. This bit set specifies to use the contents of the Length Registers as the length of the message; this bit clear specifies to use the Size field as the length of the message.
18	**Input DMA AutoIncrement Disable.** This bit clear specifies to increment the source address when using the PLB master interface to read in data. This bit set specifies not to increment the source address.
17	**Input DMA Enable.** This bit set specifies to read in data using the PLB master interface. This bit clear disables the PLB master read interface.
16	**Endian.** This bit set specifies that the data is in little endian format. This bit clear specifies that the data is in big endian format. Endian conversion is applied to the Input FIFO data and output hash value.
15:0	**Hash Size.** These bits specify the number of bytes to be processed. This field is initialized when this register is updated. During processing, this field is updated to reflect the number of bytes remaining to be hashed. When performing the HMAC Inner or Outer IV Generation command, this field specifies the number of bytes that are in the HMAC key.

4.2.3. HMAC Source Address Register

HMAC 1 PP Address: 0x4D
HMAC 1 PLB Address: 0x20040034

HMAC 2 PP Address: 0x6D
HMAC 2 PLB Address: 0x20050034

This 32-bit register stores the source address of the HMAC unit input data. This register is used when input DMA is enabled and the Packet Processor is disabled.

4.2.4. HMAC Destination Address Register

HMAC 1 PP Address: 0x4E
HMAC 1 PLB Address: 0x20040038

HMAC 2 PP Address: 0x6E
HMAC 2 PLB Address: 0x20050038

This 32-bit register stores the destination address of the HMAC unit output data. This register is used when output DMA is enabled.

4.2.5. HMAC Length Registers 0-1

HMAC 1 PP Addresses: 0x41, 0x42
HMAC 1 PLB Addresses: 0x20040004, 0x20040008

HMAC 2 PP Addresses: 0x61, 0x62
HMAC 2 PLB Addresses: 0x20050004, 0x20050008

These registers store the 61-bit length that specifies the total the number of bytes in the message. Length Register 0 stores the lower 32-bit of the length. Length Register 1 stores the upper 29 bits. The contents of these registers are appended to the message when the Final Block and Length Select bits of the HMAC Command/Status Register are set.

4.2.6. HMAC Outer IV Registers 0-4

HMAC 1 PP Addresses: 0x43 – 0x47
HMAC 1 PLB Addresses: 0x2004000C – 0x2004001C

HMAC 2 PP Addresses: 0x63 – 0x67
HMAC 2 PLB Addresses: 0x2005000C – 0x2005001C

When performing the HMAC Final command, these registers store the Outer IV to be used for the outer hash. When performing the HMAC Complete command, these registers store the HMAC key, which must be padded with zeroes if it is less than 128 bits (for MD5) or 160 bits (for SHA-1).

4.2.7. HMAC Hash Registers 0-4

HMAC 1 PP Addresses: 0x48 – 0x4C
HMAC 1 PLB Addresses: 0x20040020 – 0x20040030

HMAC 2 PP Addresses: 0x68 – 0x6C
HMAC 2 PLB Addresses: 0x20050020 – 0x20050030

These registers store either the Initial Value (IV) or the output hash result. These registers need to be loaded only when performing an update or final command, and in which case, either the Inner IV or intermediate result from a previous update command, as appropriate, is written to the registers. While the HMAC unit is busy processing, reading from these registers returns the hash value of the last 512-bit block.

When the HMAC unit completes processing the data, the hash value (also known as Integrity Check Value or authentication value) is stored in these registers. The final result begins with the high-order byte of Hash Register 0 and ends with the low-order byte of Hash Register 3 for MD5 and of Hash Register 4 for SHA-1. Note that byte swapping is automatically done for the final MD5 block to achieve the above result. Hash Register 4 is not used for MD5.

If output DMA is enabled, the contents of these registers are written out to the location specified by the HMAC Destination Address Register, using the PLB master write interface.

4.3. HMAC Input FIFO

HMAC 1 PLB Address: 0x20140000
HMAC 2 PLB Address: 0x20150000

The Input FIFOs of HMAC 1 and HMAC 2 may be accessed using the PLB address above. When input DMA is enabled, data is transferred into the FIFOs using the PLB master interfaces. When the Packet Processor is used, the Input FIFOs accepts data only from the RAM-based Controller, through the use of the WRITE_DATA instruction. When performing the HMAC Inner or Outer IV Generation command, the Input FIFO is used to store the HMAC key.